

THE SPORADIC GROUP J_2 HAUPTMODUL AND BELYĬ MAP

HARTMUT MONIEN

ABSTRACT. Determining Fourier coefficients of modular forms of a finite index noncongruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ is still a non-trivial task [1]. In this brief note we describe a new algorithm to reliably calculate an approximation for a modular form of a given weight. As an example we calculate the hauptmodul and Belyĭ map of a genus zero subgroup of the modular group defined via a canonical homomorphism by the second Janko group. Our main result is the field of definition of its Belyĭ map and the Fourier coefficients of its hauptmodul.

1. INTRODUCTION

In their paper on noncongruence subgroups Atkin and Swinnerton-Dyer [2] gave a description of a practical computational algorithm to obtain numerical approximations to modular forms. Their ideas were further developed by Hejhal [3], Strömberg [4], Booker, Strömbergson and Venkatesh [5] to calculate Maass waveforms and by Selander and Strömbergson [6] to calculate a Belyĭ map [18, 19].

In this brief note we describe an iterative algorithm based on these ideas to calculate values of modular functions of any finite index subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ of the modular group numerically to any given precision and use it to obtain Belyĭ maps. To demonstrate the effectiveness of the algorithm we proof the following theorem

Theorem 1. *Let $\sigma_0, \sigma_1 \in S_{100}$ be the permutation given in the appendix. Then the Janko group J_2 is generated by σ_0 and σ_1 and the triple $(\sigma_0, \sigma_1, (\sigma_0\sigma_1)^{-1})$ define up to simultaneous conjugation a subgroup Γ of the full modular group $\mathrm{PSL}_2(\mathbb{Z})$ with a rational Belyĭ map $\Phi : X(\Gamma) \rightarrow \mathbb{P}^1$ which obeys the equation $\Phi(z) = p_3(z)/p_c(z) = 1728 + p_2(z)/p_c(z)$ relating the branching at the elliptic points of order two and three with the polynomial p_2 , p_3 and p_c given in the accompanying material. These polynomials are defined over the number field $K = \mathbb{Q}[a]/(a^{10} - a^9 - 2a^8 + 8a^7 - 14a^6 + 35a^4 - 68a^3 + 89a^2 - 74a + 23)$ with the Galois group $\mathrm{Gal}(K/\mathbb{Q}) = S_2 \wr S_5$ of order 3840 and discriminant $3^6 5^3 7^8$.*

Proof. It is easy to check that the permutations σ_0 and σ_1 fulfil the defining relations of the Janko group J_2 , $\sigma_0^2 = \sigma_1^3 = (\sigma_0\sigma_1)^7 = (\sigma_0\sigma_1\sigma_0\sigma_1^2)^{12} = 1$. The theorem A of Magaard [25] states which of the sporadic groups with triple $(\sigma_0, \sigma_1, (\sigma_0\sigma_1)^{-1})$ defines a subgroup Γ of $\mathrm{PSL}_2(\mathbb{Z})$ with a Riemann surface $X(\Gamma)$ of genus zero. In addition this is an admissible for the theorem of Millington [16] and therefore define (up to simultaneous conjugation) an index 100 subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$. Using theorem (3.1) of Hsu [17] it is easy to verify that the group is a noncongruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. This group has no elliptic point of order

Date: March 16, 2017.

2010 Mathematics Subject Classification. 12F12, 11F11.

Key words and phrases. Inverse Galois Problem, Belyi Maps, almost simple groups.

2 and 4 elliptic points of order 3 and 2 cusps of width 1 and 14 cusps of order 7. This defines the branching structure of the Belyĭ map $\Phi : X(\Gamma) \rightarrow \mathbb{P}^1$ and the factorization of the polynomials. Using the explicit form of the polynomials an easy calculation shows that $p_3(z)/p_c(z) = 1728 + p_2(z)/p_c(z)$ which completes the proof. \square

A number of major improvements make the algorithm numerically stable and efficient enough to use arbitrary precision arithmetic. The new ideas are: using domain decomposition techniques for the modular tessellation, fast Fourier transform to precondition the resulting linear system, Krylov subspace methods to solve the resulting linear equations iteratively. The algorithm can easily be extended to calculate cusp forms and vector valued modular forms. We have implemented our algorithm in *Haskell* [7] which allows to easily write generic arbitrary precision code and to parallelize the domain decomposition.

The determination of large zero Belyĭ maps is in general a difficult problem [9]. The subject has recently attracted interest and some substantial results were obtained for genus zero Belyi maps of degree up to 250 [10], the HS sporadic group [11], for Hurwitz groups [12] and composite genus 1 Belyi maps [13]. For a detailed review of previously known methods and some new techniques and results see [14] and my lecture at the Euler Institute 2014 [15] for a more detailed account of complex analytic methods.

2. BASIC SETUP

Let $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ be the projective special linear group over \mathbb{Z} acting on the complex upper half plane $\mathcal{H} = \{x + iy \in \mathbb{C} \mid y > 0\}$ by Möbius transformations $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathcal{H} \rightarrow \mathcal{H}, \quad z \mapsto \gamma z = \frac{az + b}{cz + d}.$$

Let G be a finitely presented group and H a finite index subgroup of G . The generators of G induce a permutation of the right coset $H \backslash G$. Then the group H is determined up to isomorphism by the permutations induced by the action of the generators of G on the right coset $H \backslash G$. This fact allows for the classification of all finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. A theorem by Millington [16] states that up to simultaneous conjugation there is a one to one correspondence between triples of permutations $\{(\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3 \mid \sigma_0^2 = \sigma_1^3 = \sigma_0 \sigma_1 \sigma_\infty = id\}$ with the finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ where S_d is the symmetric group of d objects (in this case cosets). Let $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ be a finite index subgroup of the modular group of index d defined by a triple of permutations as above. If Γ contains $\{\gamma \in \mathrm{PSL}_2(\mathbb{Z}) \mid \gamma = \pm I_2 \bmod N\}$ for some fixed integer, N , it is called a congruence subgroup otherwise it is called a noncongruence subgroup. Both cases can be distinguished easily by testing relations of the generators [17]. A fundamental domain $\mathcal{F}(\Gamma)$ of Γ is a subset of \mathcal{H} such that for all $z \in \mathcal{H}$ there is exactly one element $\gamma \in \Gamma$ for which $\gamma z \in \mathcal{F}(\Gamma)$. Here we choose $\mathcal{F} = \{z = x + iy \in \mathbb{C} \mid x \in [-1/2, 1/2), |z| \geq 1\}$ as fundamental domain for the full modular group. Since Γ is a subgroup of finite index d we have $\mathrm{PSL}_2(\mathbb{Z}) = \cup_{i=1}^d \Gamma \gamma_i$ where $\{\gamma_1, \gamma_2 \dots \gamma_d\} \subset \mathrm{PSL}_2(\mathbb{Z})$ is a list of right coset representatives which implies that $\mathcal{F}(\Gamma) = \cup_{i=1}^d \gamma_i \mathcal{F}$ is a fundamental domain of Γ .

In general Γ will contain a number of finite index subgroups of the Borel subgroup with fix points in $\mathbb{P}^1(\mathbb{Q})$ called cusps. Two cusps related by a $\gamma \in \Gamma$ are called equivalent. Each cycle of σ_∞ gives rise to a cusp (equivalence class) with the corresponding cusp width being defined as the length of the cycle. Let $k \in \{0, \dots, \kappa\}$ enumerate the cycles and let $\{x_0, x_1 \dots x_\kappa\}$

be a list of unique inequivalent cusp representatives and w_k be the width of cusp x_k . Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ be the extended complex upper half plane. A modular function is a complex valued function that extends to a meromorphic function on the compactified upper half plane $f : \mathcal{H}^* \rightarrow \mathbb{C}$ satisfying $f(\gamma z) = f(z)$ for every γ and every $z \in \mathcal{H}$. The genus of Γ is defined to be the genus of the Riemann surface $X(\Gamma) = \Gamma \backslash \mathcal{H}^*$. Here we focus on the genus zero case where the field of modular functions is generated by one modular function usually called hauptmodul. We choose one of the cusps with the smallest cusp width, w_0 , as principal cusp and fix the generator $j_\Gamma : \mathcal{H}^* \rightarrow \mathbb{C}$ uniquely by imposing a growth condition on it so that as $y \rightarrow \infty$ it grows like $j_\Gamma(z = x + iy) = q^{-1} + 0 + O(q)$ where $q = \exp(2\pi iz/w_0)$ and stays finite at all the other cusps. The rational map $\Phi : X(\Gamma) \rightarrow \mathbb{P}^1$ is of degree d and a famous theorem by Belyĭ [18, 19] asserts that it can be defined up to isomorphism over $\overline{\mathbb{Q}}$. Once $j_\Gamma(z)$ is determined fix an explicit representation of Φ relating the modular $j : \mathcal{H} \rightarrow \mathbb{C}$ invariant of the full modular group to j_Γ so that we have $\Phi(j_\Gamma(z)) = j(z)$ for all $z \in \mathcal{H}$. We choose the normalization of the modular j invariant such that at the elliptic point of order two the modular invariant takes on the value $j(i) = 1728$ and vanishes at the elliptic point of order three $j((1 + i\sqrt{3})/2) = 0$.

Let k enumerate the cusps with $k = 0$ being the principal cusp. Define $\nu_0 = T^{w_0}$ where

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and for the remaining cusps $x_k = (p, q)$, with $\gcd(p, q) = 1$, pick a fixed p' from the solutions of the congruence $pp' = -1 \pmod{q}$ to define [20]

$$\nu_k = \begin{pmatrix} -p' & -(pp' + 1)/q \\ q & -p \end{pmatrix}.$$

It is easy to see that ν_k sends x_k to infinity and $\nu_k^{-1}T\nu_k$ stabilizes x_k . The modular function can therefore be expanded at each cusp in a Poincaré series [20, 6]

$$j_\Gamma(z) = \sum_{m=\mu_k}^{\infty} a_m^{(k)} q_k^m \tag{2.1}$$

with $\mu_0 = -1$ and $\mu_k = 0$ for $k > 0$, $q_k = \exp(2\pi iz'/w_k)$, $z' = \nu_k z$ and (unknown) Fourier coefficients $a_m^{(k)}$. Here we set the principal part $a_{-1}^{(0)} = 1$, and fix the arbitrary constant term $a_0^{(0)} = 0$ in agreement with the growth condition. The Fourier coefficients are known to have at most polynomial growth with m . The Poincaré series for different cusps are obviously not independent. Modular transformations $\gamma \notin \Gamma$ act transitively on the cusps. Zuckerman [20] used this fact to generate linear relations between the expansions on different cusps for general finite index subgroup $\Gamma \subset \text{PSL}_2(\mathbb{Z})$.

3. DESCRIPTION OF THE NUMERICAL ALGORITHM

From an numerical analysis point of view determining a numerical approximation for a modular function is equivalent to solving two Laplace equations for two real functions on an infinitely extended domain with complicated “periodic” boundary conditions (coming from the generators of the finite index subgroup). Domain decomposition is a technique for the large scale numerical solution of boundary value problems of elliptic partial differential

equations. It goes back to an 1870 paper by H. Schwarz [21] and is one of several constructive techniques of conformal mapping he developed for the uniformization problem. The basic idea is to solve a Dirichlet problem for an elliptic partial differential equation on a complicated domain by decomposing it into simpler overlapping domains on which the Dirichlet problem is easily solved. Its convergence for general second order differential equations has been proven by Mihlin[24] for very general domains. We now explain how to apply these ideas to the calculation of modular functions.

For each cusp with label k we define a domain \mathcal{F}_k of the complex upper half plane by

$$\mathcal{F}_k = \{x + iy \in \mathbb{C} \mid x \in [-1/2, w_k - 1/2), y \in [1/2, \infty)\}.$$

At this point the important observation here is that the preimage of $\cup_k \nu_k^{-1} \mathcal{F}_k$ form an overlapping domain decomposition of the fundamental domain $\mathcal{F}(\Gamma)$. The domain \mathcal{F}_k contains the cosets of the cycle (cusp) k as well as parts of its neighboring cosets determined by σ_0 and σ_1 . We solve the Laplace equation in the domain \mathcal{F}_k . The periodic boundary conditions and the boundary condition as $y \rightarrow \infty$ are taken care of by the particular form of the Fourier expansion. The Dirichlet boundary condition is given by the values of the hauptmodul calculated at the lower boundary of the domain which are determined by the expansions in the domains $\mathcal{F}_{k'}$ with $k' \neq k$ and the upper boundary. We approximate the modular function by a truncated expansions

$$j_\Gamma^{(k)}(z) = \sum_{m=\mu_k}^{N_k} a_m^{(k)} q_k^m \quad (3.1)$$

where we choose $N_k = Nw_k$ with N fixed. Suppose now that we already have obtained some approximation for the Fourier coefficients at all cusps. For any given z in \mathcal{H} we can determine algorithmically a unique coset representative γ_j such that $\gamma_j z \in \mathcal{F}$. The label l can be found uniquely in one of the cycles of σ_∞ , say in cycle k , since the permutation group generated by σ_0 and σ_1 acts transitively. Then we approximate $j_\Gamma(z)$ by $j_\Gamma^{(k)}(z)$. For each k we evaluate the approximate modular function according to the procedure outlined above at points $z_j^k = \nu_k^{-1}(w_k j/M + i/2 - 1/2)$ for $j \in \{0, 1, \dots, M-1\}$ where M is chosen such that M is a power of two with integer exponent and $M > 2 \times Nw_k$. The first condition ensures that we can use the simplest form of fast Fourier transform to obtain the Fourier coefficients while the second condition avoids aliasing effects. We then apply FFT to determine the expansion coefficients of $j_\Gamma^{(k)}$ for every domain. This completes one step of the domain decomposition iteration. We can view the procedure as iterative solution of the linear equations for the Fourier coefficients with the inhomogeneous part arising from the principal cusp. The rate of convergence is determined by the largest eigenvalue of the (linear) iteration operator which is less than one if the overlap of the domains is finite [24] which implies linear convergence. We observe linear convergence when using the simple (Picard) iteration. The advantage of the procedure described above is that convergence is guaranteed and it can easily be implemented in multiprecision arithmetic [8]. A further advantage is that it can be used as a pre-conditioner for more sophisticated iterative techniques which go under the name of Krylov methods [22, 23] to solve the linear equation. Using GMRES [23] which we implemented in multiprecision we actually do observe quadratic convergence in all cases we have investigated. One important point is that compared to direct methods the operation count is substantially reduced.

REFERENCES

- [1] Li, Wen-Ching Winnie and Long, Ling and Yang, Zifeng, *Modular forms for noncongruence subgroups*, Q. J. Pure Appl. Math., **1** (2005) 205–221
- [2] Atkin, A. O. L. and Swinnerton-Dyer, H. P. F., *Modular forms on noncongruence subgroups*, Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968), Amer. Math. Soc., Providence, R.I., (1971), 1–25
- [3] Hejhal, Dennis A., *On eigenfunctions of the Laplacian for Hecke triangle groups*, Emerging applications of number theory (Minneapolis, MN, 1996), IMA Vol. Math. Appl., **109** (1999), 291–315
- [4] Strömberg, Fredrik, *Hecke operators for Maass waveforms on $\mathrm{PSL}(2, \mathbb{Z})$ with integer weight and eta multiplier*, International Mathematics Research Notices. IMRN, **18** (2007), 1073–7928,
- [5] Booker, Andrew R. and Strömbergsson, Andreas and Venkatesh, Akshay, *Effective computation of Maass cusp forms*, Int. Math. Res. Not., (2006) 1073–7928
- [6] Selander, Björn and Strömbergsson, Andreas, *Sextic coverings of genus two which are branched at three points*, preprint <http://www2.math.uu.se/~astrombe/papers/g2.ps>
- [7] Haskell, *An advanced, purely functional programming language*, <https://www.haskell.org>
- [8] We use in particular the Haskell bindings *hmpfr* (available at <https://hackage.haskell.org/package/hmpfr>) of the GNU MPFR library, <http://www.mpfr.org>
- [9] Lando, Sergei K. and Zvonkin, Alexander K., *Graphs on surfaces and their applications*, With an appendix by Don B. Zagier, Low-Dimensional Topology, II, Springer-Verlag, Berlin, (2004)
- [10] Barth, Dominik and Wenz, Andreas, *Explicit Belyi maps over Q having almost simple primitive monodromy groups*, preprint <http://lanl.arxiv.org/abs/1703.02848>
- [11] Barth, Dominik and Wenz, Andreas, *Explicit Polynomials Having the Higman-Sims Group as Galois Group over $Q(t)$* , preprint <http://lanl.arxiv.org/abs/1611.04314>
- [12] Roberts, David P., *Hurwitz-Belyi Maps* preprint <http://lanl.arxiv.org/abs/1608.08302>
- [13] Vidunas, Raimundas, *Composite Genus One Belyi Maps* preprint <http://lanl.arxiv.org/abs/1610.08075>
- [14] Sijsling, J. and Voight, J., *On computing Belyi maps*, Numéro consacré au trimestre “Méthodes arithmétiques et applications”, automne 2013, Publ. Math. Besançon Algèbre Théorie Nr. **2014/1**, (2014), 73–131
- [15] Monien, H., *How to calculate rational coverings for subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ efficiently* *Embedded graphs*, <http://www.pdmi.ras.ru/EIMI/2014/EG/index.html>
- [16] Millington, M. H., *Subgroups of the classical modular group*, J. London Math. Soc. (2), **1** (1969), 351–357,
- [17] Hsu, Tim, *Identifying congruence subgroups of the modular group*, Proc. Amer. Math. Soc., **124** (1996) 1351–1359
- [18] Belyĭ, G. V., *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat., **43** (1979), 267–276, 479,
- [19] Belyĭ, G. V., *A new proof of the three-point theorem*, Mat. Sb., **193**, (2002), 21–24,
- [20] Zuckerman, Herbert S., *On the coefficients of certain modular forms belonging to subgroups of the modular group*, Trans. Amer. Math. Soc. **45** (1939) 298–321
- [21] Schwarz, H. A., *Ueber einen Grenzübergang durch alternirendes Verfahren*, Vierteljahresschrift der Naturforschenden Gesellschaft in Zürich, **15** (1870), 272–286
- [22] Trefethen, Lloyd N. and Bau, III, David, *Numerical linear algebra*, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, (1997)
- [23] Saad, Yousef, *Iterative methods for sparse linear systems*, Society for Industrial and Applied Mathematics, Philadelphia, PA, (2003)
- [24] Mihlin, S. G., *On the algorithm of Schwarz*, Doklady Akad. Nauk SSSR (N.S.), **77** (1951) 569–571
- [25] Magaard, K., *Monodromy and sporadic groups* Comm. Algebra **21** (1993), 4271–4297
- [26] Atlas database of finite groups, <http://brauer.maths.qmul.ac.uk/Atlas/v3/>
- [27] SageMath 7.5.1 (2017), <http://www.sagemath.org>

4. APPENDIX

The permutations of Theorem (1) are defined by (data from the Atlas finite groups [26]):

$$\begin{aligned}
 \sigma_0 &= (1, 84)(2, 20)(3, 48)(4, 56)(5, 82)(6, 67)(7, 55)(8, 41)(9, 35)(10, 40) \\
 &\quad (11, 78)(12, 100)(13, 49)(14, 37)(15, 94)(16, 76)(17, 19)(18, 44)(21, 34) \\
 &\quad (22, 85)(23, 92)(24, 57)(25, 75)(26, 28)(27, 64)(29, 90)(30, 97)(31, 38) \\
 &\quad (32, 68)(33, 69)(36, 53)(39, 61)(42, 73)(43, 91)(45, 86)(46, 81)(47, 89) \\
 &\quad (50, 93)(51, 96)(52, 72)(54, 74)(58, 99)(59, 95)(60, 63)(62, 83)(65, 70) \\
 &\quad (66, 88)(71, 87)(77, 98)(79, 80) \\
 \sigma_1 &= (1, 80, 22)(2, 9, 11)(3, 53, 87)(4, 23, 78)(5, 51, 18)(6, 37, 24)(8, 27, 60) \\
 &\quad (10, 62, 47)(12, 65, 31)(13, 64, 19)(14, 61, 52)(15, 98, 25)(16, 73, 32) \\
 &\quad (17, 39, 33)(20, 97, 58)(21, 96, 67)(26, 93, 99)(28, 57, 35)(29, 71, 55) \\
 &\quad (30, 69, 45)(34, 86, 82)(38, 59, 94)(40, 43, 91)(42, 68, 44)(46, 85, 89) \\
 &\quad (48, 76, 90)(49, 92, 77)(50, 66, 88)(54, 95, 56)(63, 74, 72)(70, 81, 75) \\
 &\quad (79, 100, 83)
 \end{aligned}$$

The polynomials p_2 , p_3 and p_c can be found in the data files “p2.txt”, “p3.txt” and “pc.txt” accompanying the paper.

BETHE CENTER, UNIVERSITY BONN, NUSSALLEE 12, 53115 BONN, GERMANY
E-mail address: hmonien@uni-bonn.de